JOURNAL OF ALGEBRA **182,** 653–663 (1996)
ARTICLE NO. 0194

On Product-Equality-Preserving Mappings in Groups

Gadi Moran

Department of Mathematics and Computer Science, The University of Haifa, Haifa 31905, Israel

Communicated by Leonard Lipshitz

Received March 13, 1995

Let G, H be groups, $M \subseteq G$. A mapping $f: M \to H$ is called a *Product-equality-preserving* (PEP) *mapping* iff it satisfies

$$\forall a, b, c, d \in M[ab = cd \Rightarrow f(a)f(b) = f(c)f(d)]. \qquad (*)_M$$

THEOREM. Let G_1, G_2 be nonabelian groups with centers Z_1, Z_2 and let M_1, M_2 satisfy

$$G_i \setminus Z_i \subseteq M_i \subseteq G_i, \qquad i = 1, 2.$$

Let $f: M_1 \to M_2$ be a PEP mapping that maps M_1 onto M_2. Then there is an epimorphism $\varphi: G_1 \to G_2$ and $v \in Z_2$ such that for every $x \in M_1$,

$$f(x) = v\varphi(x).$$

0. INTRODUCTION

0.0. Parameters of the multiplication table of a subset M of a group G often make a useful research tool. Typically, the number $|M^2|$ of distinct entries of this table for finite M is such a parameter. On one hand, an extensive body of research deals with determination of the possible structure of M when $|M^2|$ is small in specific groups, e.g., the additive group of integers ([F1], [F3]). On the other hand, interesting classification theorems for groups G, where $|M^2| < |M|^2$ for every $M \subseteq G$ of a fixed finite cardinality m, are available. See [F2] for $m = 2$, [BFP] for $m = 3$, and [B], [BF], and [FS] for related topics and further references.

In comparing multiplication tables of different group subsets M, M', a bijection between M and M' that, along with its inverse, preserves product equality (i.e., a PEP bijection with PEP inverse) plays an important role. Such a mapping is called an isomorphism by Freiman in [F1] and a

0021-8693/96 $18.00

2-isomorphism in [FS]. See [B] for further remarks and open questions concerning this notion.

A convenient setting for a systematic treatment of this line of research is provided by a category that we shall denote PEP (see [J], Vol. II, Chapter 1, for basics of category theory). The objects of PEP are ordered pairs (M, G), where M is a subset of the group G. A PEP morphism from (M, G) to (M', G') is any PEP mapping $f: M \to M'$. It will be convenient to use M alone to denote the object (M, G) whenever the context allows.

Let us make some observations. We let G, H, K denote groups in the sequel, and use φ, ψ to denote group homomorphisms.

0.1. If $M_1 \subseteq G$, $M_2 \subseteq H$, $\varphi: G \to H$ is a homomorphism, and $\varphi(M_1) \subseteq M_2$, then $f := \varphi|M_1$, the restriction of φ to M_1, is a PEP mapping from M_1 to M_2.

0.2. For $h \in H$, let $h_L(h_R)$ denote left (right) multiplication by h in H. That is, $h_L, h_R: H \to H$ are defined by

$$h_L(y) = hy, \qquad h_R(y) = yh \qquad (y \in H).$$

Let $h', h'' \in H$. If $M \subseteq H$ satisfies

$$h'_L|M = h''_R|M, \tag{0.1}$$

then $f := h'_L|M = h''_R|M$ is a PEP mapping. Indeed, if $a, b, c, d \in M$ and $ab = cd$, then

$$f(a)f(b) = h'_L(a)h''_R(b) = h'abh'' = h'cdh'' = h'_L(c)h''_R(d) = f(c)f(d).$$

0.3. Let $M_1 \subseteq G$, $M_2 \subseteq H$, $h', h'' \in H$, and let $\varphi: G \to H$ be a homomorphism. We call $f: M_1 \to M_2$ the *standard* (h', φ, h'')*-PEP mapping* iff

$$f = h'_L \circ \varphi|M_1 = h''_R \circ \varphi|M_1. \tag{0.2}$$

That is, $f(x) = h'\varphi(x) = \varphi(x)h''$ for all $x \in M_1$.

By 0.1 and 0.2, f is indeed a PEP mapping whenever f is the standard (h', φ, h'')-PEP mapping.

We shall call f the *standard* (h, φ)*-PEP mapping* if $h = h' = h''$ and f is the (h', φ, h'')-PEP mapping. Thus, $f: M_1 \to M_2$ is the standard (h, φ)-PEP mapping if

$$f(x) = h\varphi(x) = \varphi(x)h \qquad (x \in M_1). \tag{0.3}$$

Notice that if $f: M_1 \to M_2$ is the standard (h', φ, h'')-PEP mapping and for some $x \in M_1$, $h'\varphi(x) = \varphi(x)h'$, then in fact $h' = h''$ and f is actually the standard (h, φ)-PEP mapping, where $h = h' = h''$.

We say that $f\colon M_1 \to M_2$ is *a standard PEP mapping* if it is the standard (h', φ, h'')-PEP mapping for some h', φ, h''.

0.4. The composition of standard PEP mappings is a standard-PEP mapping.

Indeed, if $f\colon M_1 \to M_2$ is the standard (h', φ, h'') mapping, $M_3 \subseteq K$, and $g\colon M_2 \to M_3$ is the standard (k', ψ, k'') mapping, then $gf\colon M_1 \to M_3$ is the standard $(k'\psi(h'), \psi\varphi, \psi(h'')k'')$-PEP mapping. Indeed, for $x \in M_1$,

$$gf(x) = g(h'\varphi(x)) = k'\psi(h'\varphi(x)) = (k'\psi(h'))\psi\varphi(x),$$
$$gf(x) = g(\varphi(x)h'') = \psi(\varphi(x)h'')k'' = \psi\varphi(x)(\psi(h'')k'').$$

Similarly, if $f\colon M_1 \to M_2$ is the standard (h, φ) mapping, $g\colon M_2 \to M_3$ is the standard (k, ψ) mapping, and $k\psi(h) = \psi(h)k$, then gf is the standard $(k\psi(h), \psi\varphi)$-PEP mapping.

0.5. If $f\colon M_1 \to M_2$ is the standard (h_1, φ, h_2)-PEP mapping, $\varphi\colon G \to H$ is a group isomorphism (so that f is one to one), and f maps M_1 onto M_2, then $f^{-1}\colon M_2 \to M_1$ is also a PEP mapping. In fact, it is the standard $(\varphi^{-1}(h_1^{-1}), \varphi^{-1}, \varphi^{-1}(h_2^{-1}))$-PEP mapping, as one readily checks.

Similarly, if $f\colon M_1 \to M_2$ is the standard (h, φ)-PEP mapping, $\varphi\colon G \to H$ is an isomorphism (so that f is one to one), and f maps M_1 onto M_2, then the bijection $f^{-1}\colon M_2 \to M_1$ is also a PEP mapping, and, in fact, it is the standard $(\varphi^{-1}(h^{-1}), \varphi^{-1})$-PEP mapping.

0.6. Let $M \subseteq G$ satisfy

$$\forall a, b, c, d \in M[ab = cd \Rightarrow a = c \,\&\, b = d]. \qquad (0.4)_M$$

Then any $f\colon M \to H$ is a PEP mapping, as $(*)_M$ holds trivially.

It follows that the inverse of a PEP bijection is not, in general, a PEP mapping.

$(0.4)_M$ holds, for instance, when M freely generates G or when $M = \{(a, y)\colon y \in Y\}$ is a set of (distinct) transpositions, all moving the element a, and G is a group of permutations of a set containing $\{a\} \cup Y$, including M.

In contrast with 0.6, we have the following two theorems. The first theorem was proved by Freiman [F3].

THEOREM 1. *Let G, H be groups. Then for every* PEP *mapping f on G into H there is a homomorphism $\varphi\colon G \to H$ and $v \in H$ centralizing $\varphi(M)$ such that*

$$f(x) = v\varphi(x) \qquad (x \in M).$$

Let us say that $M \subseteq G$ is *cocentral in* G iff $G \setminus Z(G) \subseteq M$, where $Z(G) := \{v \in G: \forall x \in G[vx = xv]\}$ is the center of G.

Our main result is:

THEOREM 2. *Let* G_1, G_2 *be nonabelian groups and let* $M_i \subseteq G_i$ *be cocentral in* G_i, $i = 1, 2$. *Then for every* PEP *mapping* f *of* M_1 *onto* M_2 *there is an epimorphism* $\varphi: G_1 \to G_2$ *and* $v \in Z(G_2)$ *such that*

$$f(x) = v\varphi(x) \qquad (x \in M_1).$$

Theorems 1 and 2 are proved in Sections 1 and 2, respectively. The argument for Theorem 1 in Section 1 is the one we used in June 1993, en route toward the proof of Theorem 2 and unaware of Freiman's work [F3]. It is included here for the reader's convenience, as we feel it is a useful introductory vehicle for the more delicate argument presented for Theorem 2 in Section 2.

Corollaries

0.7. By Theorem 1, the group of PEP bijections of a group G is the subgroup of S_G, the symmetric group on the set G, generated by the group $\mathrm{Aut}(G)$ of automorphisms of the group G and the set $\{v_L: v \in Z(G)\}$ of (left) translations by central elements of G. Thus it is a subgroup of the holomorph $\mathrm{Hol}(G)$ generated in S_G by $\mathrm{Aut}(G)$ and the set of left translations $\{g_L: g \in G\}$ (see [J], Vol. I, 1.10).

In particular:

0.8. If G is abelian, then the group of PEP bijections of G is $\mathrm{Hol}(G)$.

0.9. If G is nonabelian with center Z, then for every cocentral M in G, the group of PEP bijections of M is isomorphic to the group of standard PEP bijections of G mapping M onto M. In fact $f \mapsto f|M$ is such an isomorphism, by Theorem 2.

2. PROOF OF THEOREM 1

We assume in this section that G, H are groups and $f: G \to H$. We call f a PEP mapping iff $(*)_G$ is satisfied, i.e.,

$$\forall a, b, c, d \in G[ab = cd \Rightarrow f(a)f(b) = f(c)f(d)]. \qquad (1.0)$$

We let 1 denote the identity element of G.

1.1. *The following are equivalent*:

(i) *f is a PEP mapping, i.e.,* (1.0) *holds.*

(ii) $f(abc^{-1}) = f(a)f(b)f(c)^{-1}$ *for all* $a, b, c \in G$.

(iii) $f(ab)f(1) = f(a)f(b)$ *for all* $a, b \in G$.

Proof. (i) $\Rightarrow$ (ii): Assume (1.0) and let $a, b, c \in G$. As $(abc^{-1})c = ab$, we have $f(abc^{-1})f(c) = f(a)f(b)$ and so (ii) holds.

(ii) $\Rightarrow$ (iii): Assume (ii) and let $a, b \in G$. By (ii), $f(ab) = f(ab1^{-1}) = f(a)f(b)f(1)^{-1}$ and so (iii) holds.

(iii) $\Rightarrow$ (i): Assume (iii) and let $a, b, c, d \in G$ satisfy $ab = cd$. Then by (iii),

$$f(a)f(b) = f(ab)f(1) = f(cd)f(1) = f(c)f(d).$$

Thus, (i) holds. ∎

1.2. *Let $f\colon G \to H$ be a* PEP *mapping. Then $f(1) \in H$ centralizes $f(G)$, i.e.,*

$$f(g)f(1) = f(1)f(g) \qquad \text{for all } g \in G. \tag{1.1}$$

Proof. Indeed, by 1.1(iii),

$$f(g)f(1) = f(1 \cdot g)f(1) = f(1) \cdot f(g).$$ ∎

1.3. *Let $f\colon G \to H$ be a PEP mapping and define $\varphi\colon G \to H$ by*

$$\varphi(g) := f(1)^{-1}f(g).$$

Then $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$, i.e., φ is a homomorphism.

Proof. By 1.1 and 1.2, we have

$$\begin{aligned}\varphi(xy) &= f(1)^{-1}f(xy) = f(1)^{-2}f(1)f(xy) = f(1)^{-2}f(xy)f(1)\\ &= f(1)^{-2}f(x)f(y) = \big(f(1)^{-1}f(x)\big)\big(f(1)^{-1}f(y)\big) = \varphi(x)\varphi(y).\end{aligned}$$ ∎

Proof of Theorem 1. Let $f\colon G \to H$ be a PEP mapping. Define $\varphi\colon G \to H$, $v \in H$, by

$$\varphi(x) = f(1)^{-1}f(x), \qquad v = f(1).$$

Then $f(x) = v\varphi(x)$ and by, 1.2 and 1.3, φ is a homomorphism and v centralizes $\varphi(G)$. Theorem 1 is proved. ∎

2. PROOF OF THEOREM 2

We assume in this section that G_1, G_2 are nonabelian groups with centers Z_1, Z_2, M_i is a cocentral subset of G_i, i.e., $G_i \setminus Z_i \subseteq M_i \subseteq G_i$, $i = 1, 2$, and f: $M_1 \to M_2$ is a PEP mapping of M_1 *onto* M_2, i.e.,

$$\forall a, b, c, d \in M_1 \big[ab = cd \Rightarrow f(a)f(b) = f(c)f(d) \big]. \tag{2.0}$$

Under these assumptions, we prove:

THEOREM 2.0. *There is an epimorphism* φ: $G_1 \to G_2$ *of* G_1 onto G_2 *and an element* $v \in Z_2$ *such that*

$$\forall x \in M_1 \big[f(x) = v\varphi(x) \big]. \tag{2.1}$$

Let us put $M_i^0 = G_i \setminus Z_i$, so that $M_i^0 \subseteq M_i$, $i = 1, 2$.

We proceed through a series of propositions. The first lists useful properties of the sets M_i^0.

2.1. M_i^0 *satisfies for* $i = 1, 2$:

(i) $a \in M_i^0 \Leftrightarrow a^{-1} \in M_i^0$.

(ii) $c \in M_i^0 \Rightarrow \exists a, b \in M_i^0$ $[c = ab]$.

(iii) $w \in Z_i$, $a \in G_i \Rightarrow [a \in M_i^0 \Leftrightarrow aw \in M_i^0]$.

(iv) *Let* $a, b \in G_i$. *Then* $ab \in Z_i \Rightarrow ab = ba$.

Proof. Recall that $a \in M_i^0$ if $\exists x \in G[xa \neq ax]$. Hence;

(i) Follows from $xa \neq ax \Leftrightarrow a^{-1}x = a^{-1}(xa)a^{-1} \neq a^{-1}(ax)a^{-1} = xa^{-1}$.

(ii) Let $b, c \in G_i$, $cb \neq bc$. Thus $b, c \in M_i^0$ and $c = (cb^{-1})b$. Let $a = cb^{-1}$. Then $c = ab$ and $b \in M_i^0$. Also, $a \in M_i^0$ as by $cb \neq bc$ we have $ba = bcb^{-1} \neq cbb^{-1} = c = cb^{-1}b = ab$.

(iii) Indeed, M_i^0 is a union of the cosets aZ_i in G_i other than Z_i.

(iv) Let $a, b \in G_i$. As $b(ab)b^{-1} = ba$, we see that $ab = ba$ whenever ab commutes with b. Thus, if $ab \in Z_i$ certainly $ab = ba$. ∎

2.2. (i) $M_2^0 \subseteq f(M_1^0)$.

(ii) *There is a* $u \in Z_2$ *such that*

$$a, a^{-1} \in M_1 \Rightarrow f(a)f(a^{-1}) = f(a^{-1})f(a) = u. \tag{2.2}$$

Proof. (i) Let $c \in M_2^0 \subseteq M_2$ and let $d \in M_2$ satisfy $cd \neq dc$. As f maps M_1 onto M_2, there are $a, b \in M_1$ such that $f(a) = c$ and $f(b) = d$. By (2.0), $ab \neq ba$ (else $cd = dc$) so that $a, b \notin Z_1$, i.e., $a, b \in M_1^0$. Hence $c = f(a) \in f(M_1^0)$ and we have $M_2^0 \subseteq f(M_1^0)$.

(ii) $M_1^0 \neq \phi$, so let $a_0 \in M_1^0$. By 2.1(i), $a_0^{-1} \in M_1^0$ as well. Put

$$u := f(a_0)f(a_0^{-1}).$$

Let now $a, a^{-1} \in M_1$. As

$$aa^{-1} = a^{-1}a = a_0a_0^{-1},$$

we obtain, by (2.0),

$$f(a)f(a^{-1}) = f(a^{-1})f(a) = u$$

and so (2.2) holds.

We show that $u \in Z_2$. Let $a \in M_1^0$. By (2.2), we have $f(a^{-1}) = uf(a)^{-1} = f(a)^{-1}u$, so u commutes with $f(a)^{-1}$ for all $a \in M_1^0$. By 2.1(i), u commutes with $f(a)$ for every $a \in M_1^0$, i.e., u centralizes $f(M_1^0)$. But $M_2^0 \subseteq f(M_1^0)$ by (i), and so u centralizes $M_2^0 = G_2 \setminus Z_2$, whence $u \in Z_2$. ∎

2.3. *Let $a, b, c \in M_1$. We have*:

(i) $a^{-1} \in M_1 \Rightarrow f(a^{-1})^{-1} = u^{-1}f(a) = f(a)u^{-1}$.

(ii) $abc^{-1} \in M_1 \Rightarrow f(abc^{-1}) = f(a)f(b)f(c)^{-1}$.

(iii) $abc, c, c^{-1} \in M_1 \Rightarrow f(abc) = u^{-1}f(a)f(b)f(c)$.

Proof. (i) By 2.2(i) $f(a)f(a^{-1}) = f(a)f(a^{-1}) = u \in Z_2$, whence

$$f(a^{-1})^{-1} = u^{-1}f(a) = f(a)u^{-1}$$

(ii) By (2.0) and $(abc^{-1})c = ab$, we have

$$f(abc^{-1})f(c) = f(a)f(b) \qquad \text{or} \qquad f(abc^{-1}) = f(a)f(b)f(c)^{-1}.$$

(iii) By (ii) and (i), we have

$$\begin{aligned} f(abc) &= f\left(ab(c^{-1})^{-1}\right) = f(a)f(b)f(c^{-1})^{-1} \\ &= f(a)f(b)f(c)u^{-1} = u^{-1}f(a)f(b)f(c). \end{aligned}$$

∎

2.4. *There is a $v \in Z_2$ such that*

$$a, b, ab, (ab)^{-1} \in M_1 \Rightarrow v = f(a)f(b)f(ab)^{-1} = f(ab)^{-1}f(a)f(b). \tag{2.3}$$

We split the proof of 2.4 *into steps*:

2.4.1. *Let* $a, b, ab, (ab)^{-1}, \tilde{a}, \tilde{b}, \tilde{a}\tilde{b}, (\tilde{a}\tilde{b})^{-1} \in M_1$. *Then*

$$f(a)f(b)f(\tilde{a}\tilde{b}) = f(ab)f(\tilde{a})f(\tilde{b}). \tag{2.4}$$

Proof. Indeed, let $c = ab\tilde{a}\tilde{b} = ab(\tilde{a}\tilde{b}) = (ab)\tilde{a}\tilde{b}$. By 2.3(iii),

$$f(c) = u^{-1}f(a)f(b)f(\tilde{a}\tilde{b}) = u^{-1}f(ab)f(\tilde{a})f(\tilde{b}).$$

(2.4) follows. ∎

2.4.2. *Let* $a, b, ab, (ab)^{-1} \in M_1$. *Then*

$$f(a)f(b)f(ab)^{-1} = f(ab)^{-1}f(a)f(b).$$

Proof. Put $a = \tilde{a}$ and $b = \tilde{b}$ in 2.4.1. ∎

2.4.3. *Let* $a, b, ab, (ab)^{-1}, \tilde{a}, \tilde{b}, \tilde{a}\tilde{b}, (\tilde{a}\tilde{b})^{-1} \in M_1$. *Then*

$$f(a)f(b)f(ab)^{-1} = f(\tilde{a})f(\tilde{b})f(\tilde{a}\tilde{b})^{-1}. \tag{2.5}$$

Proof. By 2.4.1, (2.4) holds. Hence

$$f(ab)^{-1}f(a)f(b) = f(\tilde{a})f(\tilde{b})f(\tilde{a}\tilde{b})^{-1}.$$

By 2.4.2, (2.5) holds. ∎

2.4.4. *Let* $a_0, b_0, a_0b_0 \in M_1^0$ *and let*

$$v := f(a_0)f(b_0)f(a_0b_0)^{-1}.$$

Then $v \in Z_2$.

Proof. Let $d \in M_2^0$. By 2.2(i), there is a $c \in M_1^0$ with $f(c) = d$ and, by 2.1(ii), there are $a, b \in M_1^0$ with $c = ab$. By 2.1(i), $c^{-1} = (ab)^{-1} \in M_1^0$ and also $(a_0b_0)^{-1} \in M_1^0$.
Thus, by 2.4.3 and 2.4.2

$$v = f(a_0)f(b_0)f(a_0b_0)^{-1} = f(a)f(b)f(ab)^{-1} = f(ab)^{-1}f(a)f(b),$$

i.e., $v = f(a)f(b)d^{-1} = d^{-1}f(a)f(b)$, whence $f(a)f(b) = dv = vd$. Thus, v centralizes M_2^0, and so $v \in Z_2$. ∎

Proof of 2.4. As $M_1^0 \neq \phi$, 2.2(i) and (ii) guarantee the existence of $a_0, b_0 \in M_1^0$ such that also $a_0b_0 \in M_1^0$, hence also $(a_0b_0)^{-1} \in M_1^0$. Use

a_0, b_0 to define $v \in G_2$ as in 2.4.4. By 2.4.1–2.4.4, $v \in Z_2$, and whenever $a, b, ab, (ab)^{-1} \in M_2$, we have

$$v = f(a)f(b)f(ab)^{-1} = f(ab)^{-1}f(a)f(b). \quad \blacksquare$$

2.5. *Let* $w \in Z_1$, $aw, a, a^{-1}, bw, b, b^{-1} \in M_1$. *Then*:

(i) $f(aw)f(a)^{-1} = f(bw)f(b)^{-1}$.

(ii) $f(aw)f(a)^{-1} \in Z_2$.

(iii) $f(aw)f(a)^{-1} = f(a)^{-1}f(aw)$.

Proof. (i) As $w = (aw)a^{-1} = (bw)b^{-1}$, (2.0) implies $f(aw)f(a^{-1}) = f(bw)f(b^{-1})$. By (2.2), $f(a^{-1}) = f(a)^{-1}u$ and $f(b^{-1}) = f(b)^{-1}u$, so that $f(aw)f(a)^{-1} = f(bw)f(b)^{-1}$.

(ii) Let $d \in M_2^0$. By 2.2(i), let $c \in M_1^0$ satisfy $d = f(c)$. As $cw, c, c^{-1} \in M_1^0 \subseteq M_1$, we have, by (i), $f(aw)f(a)^{-1} = f(cw)f(c)^{-1}$. Thus $df(aw)f(a)^{-1} = df(cw)f(c)^{-1} = f(c)f(cw)f(c)^{-1}$. Hence, by 2.3(ii) and by $w \in Z_1$,

$$\begin{aligned} df(aw)f(a)^{-1} &= f(c \cdot cw \cdot c^{-1}) = f(cw) = f(wc) = f\big((aw)a^{-1}c\big) \\ &= u^{-1}f(aw)f(a^{-1})f(c) \\ &= u^{-1}f(aw)f(a)^{-1}ud = f(aw)f(a)^{-1}d, \end{aligned}$$

where the last three equalities use 2.3(iii), and 2.2(i). Thus, $f(aw)f(a)^{-1}$ centralizes M_2^0, hence $f(aw)f(a)^{-1} \in Z_2$.

(iii) $f(aw)f(a)^{-1} = f(a)^{-1}f(aw)$ follows from (ii) by 2.1(iv). $\blacksquare$

We are now ready to define the epimorphism $\varphi\colon G_1 \to G_2$ and the element $v \in Z_2$ mentioned in Theorem 2.0.

DEFINITION 2.6. Let $a_0, b_0, a_0b_0 \in M_1^0$. Define an element $v \in G_2$ and a mapping $\varphi\colon G_1 \to G_2$ as follows:

(i) $v := f(a_0)f(b_0)f(a_0b_0)^{-1}$.

(ii) $\varphi(a) := v^{-1}f(a)$ for $a \in M_1^0$.

(iii) $\varphi(w) := f(a_0w)f(a_0)^{-1}$ for $w \in Z_1$.

Two remarks are in order:

2.6.1. v *is well defined,* $v \in Z_2$, *and satisfies* (2.3).

Proof. $M_1^0 \neq \phi$, so let $c \in M_1^0$. By 2.1(ii), there are $a_0, b_0 \in M_1^0$ with $a_0b_0 = c$, and by 2.1(i), also $(a_0b_0)^{-1} = c^{-1} \in M_1^0$. $M_1^0 \subseteq M_1$, so $v = f(a_0)f(b_0)f(a_0b_0)^{-1}$ is well defined. By 2.4, 2.6.1 follows. $\blacksquare$

2.6.2. (i) $a \in M_1^0 \Rightarrow \varphi(a) = v^{-1}f(a) = f(a)v^{-1}$.
(ii) $w \in M_1 \setminus M_1^0$, $a \in M_1^0 \Rightarrow \varphi(w) = f(aw)f(a)^{-1} = f(wa)f(a)^{-1} = f(a)^{-1}f(aw) = f(a)^{-1}f(wa) \in Z_2$.

Proof. By 2.6.1 and 2.5. ∎

v of Definition 2.6 and u of 2.2 are related in the next proposition.

2.7. $u = v^2$.

Proof. Let $a, b, ab \in M_1^0$. Then also $a^{-1}, b^{-1}, (ab)^{-1} \in M_1^0$ and, by 2.6.1, 2.2, and 2.3(i),

$$\begin{aligned} v^2 &= f(a)f(b)f(ab)^{-1}f\big((ab)^{-1}\big)^{-1}f(b^{-1})f(a^{-1}) \\ &= f(a)f(b)f(ab)^{-1}u^{-1}f(ab)uf(b)^{-1}uf(a)^{-1} = u. \end{aligned}$$ ∎

2.8. $f(x) = v\varphi(x)$ *for* $x \in M_1$.

Proof. If $x = a \in M_1^0$, 2.8 holds by Definition 2.6(ii). Let $x = w \in M_1 \setminus M_1^0 = M_1 \cap Z_1$ and let $a \in M_1^0$. Then $w, a, wa, (wa)^{-1} \in M_1$, so by (2.3), $v = f(w)f(a)f(wa)^{-1}$ and by 2.6.2, $\varphi(w) = f(wa)f(a)^{-1}$. Hence $v\varphi(w) = f(w)$. ∎

2.9. $\varphi\colon G_1 \to G_2$ *is a homomorphism.*

Proof. Let $x_1, x_2 \in G_1$. We show $\varphi(x_1x_2) = \varphi(x_1)\varphi(x_2)$. Distinguish the following possible cases:

Case 1. $x_1 = a$, $x_2 = b$, $a, b, ab \in M_1^0$. By Definition 2.6(ii) and 2.6.1, we have

$$\varphi(a)\varphi(b) = v^{-1}f(a)v^{-1}f(b) = v^{-1}\big(v^{-1}f(a)f(b)\big)$$

and $v^{-1} = f(ab)f(b)^{-1}f(a)^{-1}$, so that $\varphi(a)\varphi(b) = v^{-1}f(ab) = \varphi(ab)$.

Case 2. $x_1 = a$, $x_2 = b$, $x_1x_2 = w$, $a, b \in M_1^0$, $w \in Z_1$. By Definition 2.6(iii), 2.3(i), 2.6.2(ii), and 2.7, we have

$$\begin{aligned} \varphi(ab) = \varphi(w) &= f(wb^{-1})f(b^{-1})^{-1} = f(a)u^{-1}f(b) \\ &= \big(v^{-1}f(a)\big)\big(v^{-1}f(b)\big) = \varphi(a)\varphi(b). \end{aligned}$$

Case 3. $x_1 = a$, $x_2 = w$, $a \in M_1^0$, $w \in Z_1$. As $aw \in M_1^0$, $w \in Z_1$, we have, by Definition 2.6 and 2.6.2,

$$\varphi(aw) = v^{-1}f(aw) = \big(v^{-1}f(a)\big)\big(f(a)^{-1}f(aw)\big) = \varphi(a)\varphi(w).$$

Case 4. $x_1 = w$, $x_2 = a$, $w \in Z_1$, $a \in M_1^0$. As $wa = aw$, $\varphi(w)\varphi(a) = \varphi(a)\varphi(w)$, this case follows from Case 3.

Case 5. $x_1 = w_1$, $x_2 = w_2$, $w_1, w_2 \in Z_1$. Let $a \in M_1^0$. As $w_1, w_2, w_1w_2 = w_2w_1 \in Z_1$, we have $w_2^{-1} \in Z_1$, $w_1a, w_2^{-1}a \in M_1^0$. Hence, by 2.6.2,

$$\begin{aligned}\varphi(w_1)\varphi(w_2) &= \left(f(w_1a)f(a)^{-1}\right)\left(f\left(w_2\left(w_2^{-1}a\right)\right)f\left(w_2^{-1}a\right)^{-1}\right)\\ &= f(w_1a)f\left(w_2^{-1}a\right)^{-1}\\ &= f\left(w_1w_2\left(w_2^{-1}a\right)\right)f\left(w_2^{-1}a\right)^{-1} = \varphi(w_1w_2).\end{aligned}$$

∎

2.10. *φ: $G_1 \to G_2$ is an epimorphism mapping M_1 onto $v^{-1}M_2$.*

Proof. By 2.8 and 2.9, it is left to show that φ maps G_1 onto G_2. By Definition 2.6(ii) and 2.2(i), $M_2^0 \subseteq \varphi(M_1^0)$. As $(M_2^0)^2 = G_2$, φ maps G_1 onto G_2 by 2.9. ∎

The proof of Theorem 2.0—hence of Theorem 2—is complete.

ACKNOWLEDGMENT

We are grateful to Ya. G. Berkovich for introducing us to the problem.

REFERENCES

[B] Ya. G. Berkovich, "Set Squaring in Groups," to appear.

[BFP] Ya. G. Berkovich, G. A. Freiman, and C. Praeger, Small squaring and cubing properties for finite groups, *Bull. Austral. Math. Soc.* **44** (1991), 429–450.

[BF] L. V. Brailovsky and G. a. Freiman, Groups with small cardinality of the cubes of their two-element subsets, *Ann. New York Acad. Sci.* **410** (1983), 75–82.

[F1] G. A. Freiman, "Foundation of a Structural Theory of Set Addition," Translations of Mathematical Monographs, Vol. 37, Am. Math. Soc., Providence, RI, 1973.

[F2] G. a. Freiman, On two- and three-element subsets of groups, *Aequationes Math.* **22** (1981), 140–152.

[F3] G. A. Freiman, Nonclosed semigroups with cancellation, *Ann. New York Acad. Sci.* **410** (1983), 91–98.

[FS] G. A. Freiman and B. M. Schein, Interconnections between the structure theory of set addition and rewritability in groups, *Proc. Am. Math. Soc.* **113** (1991), 899–910.

[J] N. Jacobson, Basic Algebra, 2nd. ed., Freeman, New York, 1985.